ดร.วิรินทร์ เมฆประดิษฐสิน

Networking

รอบรู้การออกแบบระบบเครือข่าย Switching

ตอนอวสาน เทคโนโลยีและแนวคิดสมัยใหม่กับการออกแบบเครือข่าย Switching

เทคโนโลยีและแนวคิดสมัยใหม่ที่มีความหลากหลายจากผู้ผลิตต่างๆ ที่เสนอ นวัตกรรมทางเทคโนโลยีใหม่ ๆ สู่ Switching Hub เพื่อเพิ่มศักย์ภาพการทำงานบนเครือข่ายที่นับวันจะมีความสลับซับซ้อนมากยิ่งขึ้น

ฉบับที่แล้วได้กล่าวถึง เทคโนโลยีและแนวคิดสมัยใหม่ที่มีความหลากหลายจากผู้ผลิตต่าง ๆ ที่เสนอนวัตกรรมทางเทคโนโลยีใหม่ ๆ สู่ Switching Hub เพื่อเพิ่มศักย์ภาพการทำงานบนเครือข่าย ที่นับวันจะมีความสลับซับซ้อนมากยิ่งขึ้น ความเข้าใจในแนวคิดและเทคโนโลยีต่าง ๆ เหล่านี้จะช่วยให้ท่านสามารถเลือกซื้อ และเข้าใจการวางตำแหน่งของ Switching Hub บนเครือข่ายได้อย่างถูกต้อง และมีประสิทธิภาพสูงสุด

ฉบับนี้จะได้กล่าวถึงวิธีการเพิ่มประสิทธิภาพของเครือข่ายโดย Switching Hub ซึ่งต่อจากฉบับที่แล้ว รวมทั้ง เทคโนโลยีของ Cisco และการออกแบบเครือข่าย Switching ฉบับมาตรฐานเป็นอันดับสุดท้าย

การเพิ่มแบนวิดธ์เครือข่ายรวมทั้งความปลอดภัยและน่าเชื่อถือ

วิธีการเพิ่มแบนวิดธ์บนเครือข่ายก็คือ การลด Broadcasting ที่เกิดขึ้นบนเครือข่ายให้น้อยที่สุดหรือให้หมดไป แม้ว่า Switching Hub โดยทั่วไป ที่เป็น Layer 2 จะช่วยเพิ่มแบนวิดธ์ให้กับเครือข่าย แต่ก็ไม่สามารถลดปัญหา Broadcasting ซึ่งกินแบนวิดธ์ของเครือข่ายลงได้ (ยกเว้น Layer 3 Switching)

การใช้ Virtual LAN (VLAN)

VLAN เป็นวิธีการจัดตั้งแลนที่ช่วยเพิ่มประสิทธิภาพของเครือข่ายเป็นอย่างมาก เนื่องจากการแบ่งผู้ใช้งานต่าง ๆ ออกเป็น VLAN ในลักษณะกลุ่มหรือ Domain จะช่วยเพิ่มประสิทธิภาพการสื่อสารภายในกลุ่ม รวมทั้งเครือข่ายโดยรวม อีกทั้งเป็นการเพิ่มความปลอดภัยให้กับกลุ่มและเครือข่ายอีกด้วย เมื่อเป็นเช่นนี้คำถามมีอยู่ว่า VLAN คืออะไร?

VLAN เป็นระบบเครือข่ายแลนแบบเสมือนที่ไม่ถูกจำกัดบนการเชื่อมต่อทางกายภาพ ซึ่งให้ประโยชน์ในด้านการลดการสูญเสียแบนวิดธ์ และเพิ่มความปลอดภัยให้กับเครือข่าย มาถึงตรงนี้ท่านผู้อ่านบางท่านอาจเริ่มงง (ผู้เขียนก็เริ่มจะงงเช่นกัน) ถ้าจะพูดแบบง่าย ๆ ก็คือ VLAN เป็นการจัดกลุ่มของผู้ใช้งานต่างๆ ที่เชื่อมต่อกันบน Switching Hub ซึ่งการจัดกลุ่มนี้จะทำให้ผู้ใช้งานที่อยู่ใน Switching Hub เดียวกัน ไม่สามารถมองเห็นกันหรือไม่สามารถสื่อสารกันได้ และหากต้องการจะสื่อสารกัน ก็ต้องใช้เราท์เตอร์จับกลุ่ม VLAN ต่าง ๆ เหล่านี้เข้ามาเชื่อมต่อกันได้ ลักษณะนี้เปรียบได้กับทุก ๆ คนอยู่ในบ้านหลังเดียวกัน แต่อยู่กันคนละห้องต่างคนต่างมีห้องของตนเอง รวมทั้งประตูเข้าออกคนละบานลักษณะนี้ผู้ที่อาศัยอยู่ในบ้านหลังนี้ จะไม่มีโอกาสได้เห็นหน้าและเสวนาระหว่างกัน ยกเว้นผู้ที่อยู่ในกลุ่ม VLAN เดียวกันเท่านั้นที่จะใช้ประตูเข้าออก รวมทั้งห้องเดียวกันที่จะสื่อสารกันได้ ซึ่งบ้านที่กล่าวมานี้เปรียบได้กับ Switching Hub ที่ทุกคนต่างก็อาศัยเพื่อการเชื่อมต่อบนเครือข่าย นั่นเอง (ดูรูปที่ 1)

การที่มีการแบ่งกลุ่มเช่นนี้ จะทำให้มีการสื่อสารเฉพาะในกลุ่มเดียวกันเท่านั้น และBroadcasting ที่เกิดขึ้นภายในกลุ่มจะไม่มีวันทะลุออกไปนอกกลุ่มโดยเด็ดขาด เมื่อเป็นเช่นนี้ก็เป็นการจำกัดบริเวณตัว Traffic ไม่ให้ออกไปรบกวนเครือข่ายโดยรวมได้ อีกทั้งยังเพิ่มความปลอดภัยให้กับเครือข่าย เนื่องจากผู้ใช้งานจากกลุ่มอื่นไม่สามารถดักจับ Packet ที่วิ่งไปมาในกลุ่มต่าง ๆ ได้ ทำให้มีความปลอดภัย

เราสามารถกล่าวได้ว่า Virtual หรือ VLAN นี้เป็น Broadcasting Domain และสาเหตุที่เรียกว่า Broadcasting Domain เนื่องจากว่า ผู้ใช้งานที่อยู่ภายใน Domain ที่ถูกกำหนดขึ้นมานี้ สามารถสื่อสารข้อมูลระหว่างกันได้เท่านั้น ไม่สามารถสื่อสารข้าม Domain กันได้ และหากการสื่อสารข้าม Domain กันก็สามารถทำได้ด้วยการใช้ Router เท่านั้น

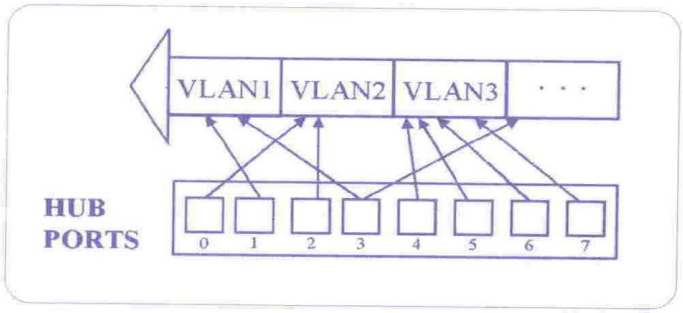
ท่านผู้อ่านอย่าเพิ่งสับสนกับความหมายระหว่าง LAN กับ VLAN ซึ่งโดยปกติทุกคนที่เชื่อมต่อกันบน Switching Hub ต่างก็เชื่อมต่อกันบนแลนอยู่แล้ว แต่ที่เรียกว่า VLAN ก็เนื่องจากมีการแบ่งจำนวนผู้ใช้งานออกเป็นกลุ่มหรือ Domain โดยที่การเชื่อมต่อบนแลนยังเหมือนเดิม เพียงแต่กระบวนการทำงานของ VLAN จะทำให้ กลุ่มของผู้ใช้งานที่ถูกแบ่งออกเป็น VLAN ต่าง ๆ จะไม่สามารถสื่อสารกันได้ตามปกติ โดยที่ลักษณะการเชื่อมต่อยังเหมือนเดิม และการจะจัดกลุ่ม VLAN กันใหม่ ก็สามารถทำได้โดยการจัด Configuration บน Switching Hub เพียงอย่างเดียวเท่านั้น ข้อเท็จจริงอีกประการหนึ่งคือระบบ VLAN ใช้ได้กับ Switching Hub เท่านั้น ไม่สามารถใช้กับ Shared Hub โดยทั่วไป

ชนิดของ VLAN

เราสามารถกำหนดชนิดของ VLAN ได้ดังนี้

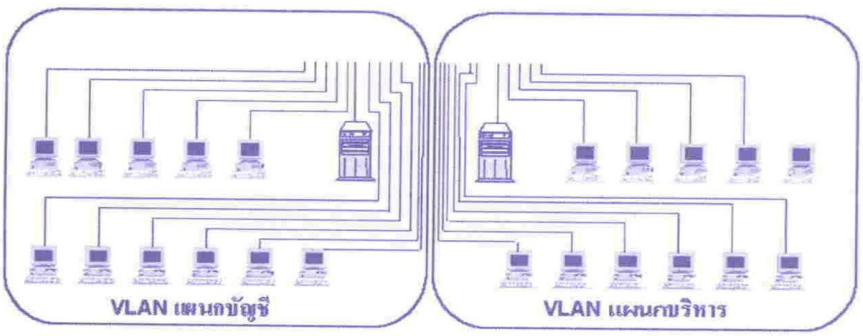
Port Group VLAN

บางครั้งก็เรียกว่า Port Based VLAN โดย VLAN ประเภทนี้ ก็เป็นชนิดของ VLAN ที่สมกับชื่อของมัน กล่าวคือ ท่านสามารถแบ่งกลุ่มของ VLAN โดยอาศัยเลขหมายของ Port ของ Switching Hub เป็นหลัก โดยมีลักษณะดังต่อไปนี้ (ดูรูปที่ 2)

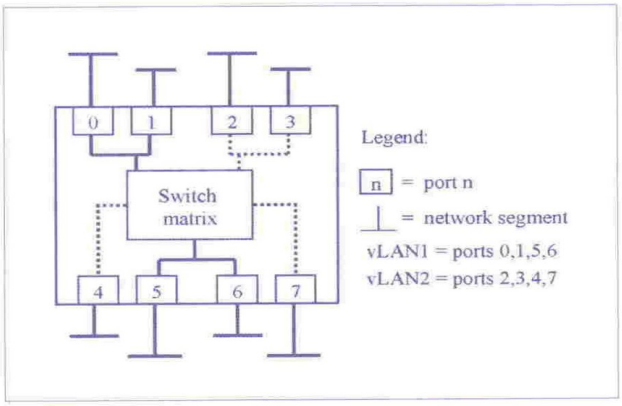


รูปที่ 2 แสดงลักษณะ Port Group VLAN

รูปที่ 1 แสดงลักษณะของ VLAN



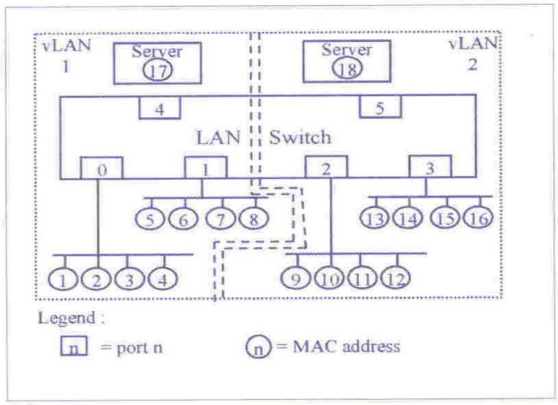
สมมติว่า Switching Hub ท่านมีอยู่ 24 Port มีผู้ใช้งาน ครบ 24 ท่าน และทั้ง 24 ท่านมาจากแผนกต่าง ๆ เช่น แผนก Accounting และแผนก Engineering สมมติว่า ต้องการจัดตั้ง VLAN ให้กับแผนก Accounting กับ Engineering ก็สามารถทำได้โดยดูว่า ผู้ใช้งานแผนก Accounting และ Engineering เชื่อมต่อที่พอร์ทใดของ Switching Hub บ้าง จากนั้นก็กำหนดให้ VLAN1 ประกอบด้วย ผู้ใช้งานจาก Accounting ที่เชื่อมต่อบนพอร์ทต่าง ๆ ของ Switching Hub ส่วนพอร์ทที่เหลือทั้งหมดให้จัดเป็น VLAN2 ไป ลักษณะนี้เราอาศัยการจัดกลุ่มของพอร์ทต่าง ๆ เป็น VLAN1 หรือ 2 ตามต้องการ อนึ่งรูปแบบของพอร์ท Group VLAN นี้ แต่ละพอร์ทจะรองรับ 1 พอร์ท ต่อ 1 Station เท่านั้น แต่ Switching Hub บางรุ่นสามารถสนับสนุนการเชื่อมต่อ 1 พอร์ท ต่อ Hub ได้ (ดูรูปที่ 3)



รูปที่ 3
แสดงการจัดกลุ่ม Port group VLAN

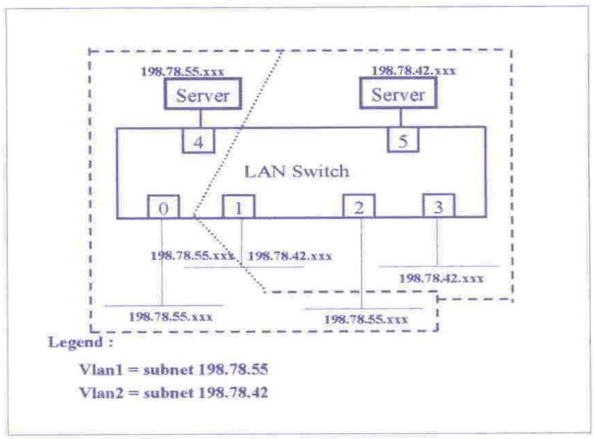
MAC Based VLAN หรือ Layer-2 VLAN

การทำงานของ VLAN ประเภทนี้ เป็นการทำงานภายใต้ Layer 2 ของ OSI Model ลักษณะของ MAC Based VLAN คือการกำหนด MAC Address เป็นสมาชิกของ VLAN แทนที่จะเป็นการกำหนดพอร์ทของ Switching Hub แต่กลับอาศัย MAC Address ของ Station ต่างๆ แทน ดังนั้น 1 พอร์ทของ Switching Hub สามารถรองรับ MAC Address ได้เป็นจำนวนมาก (1 Switching Port เชื่อมต่อกับ Shared Hub ที่มีจำนวน Port มากเท่าใด ก็จะยิ่งได้ MAC Address ค่อนข้างมากเท่านั้น) ซึ่งรูปแบบการใช้งาน MAC Based VLAN นี้มีความยืดหยุ่นดีมาก เนื่องจาก Shared Hub เดียวกันอาจประกอบด้วย ผู้ใช้งานจากแผนกต่าง ๆ (VLAN ต่าง ๆ) ก็ได้ ด้วยเหตุนี้ 1 Switching Port อาจประกอบด้วยสมาชิกจากหลาย ๆ VLAN ก็เป็นได้ ลักษณะนี้เหมาะสำหรับ รูปแบบการเชื่อมต่อที่ 1 Switching Hub Port เชื่อมต่อกับหนึ่ง Shared Hub หรือมากกว่า และสมาชิกของ VLAN ต่าง ๆ ก็สามารถมาจาก Shared Hub เดียวในพอร์ทเดียว หรือหลาย Shared Hub จากหลายๆ Port ก็เป็นได้ (ดูรูปที่ 4)



รูปที่ 4
แสดง MAC Based VLAN หรือ Layer -2 VLAN

ภาพที่ 4 แสดงให้เห็นถึงการจัด Configuration ของ MAC Based VLAN การที่จะทำเช่นนี้ได้ตัว Switching Hub หรือ Router เองจะต้องมีพอร์ทแต่ละพอร์ทที่สนับสนุน Segment ต่างๆ ได้ จากรูปที่ 4 จะเห็นว่ามีอยู่ 2 VLAN และ VLAN จะมีสมาชิก มาจาก Segment หรือ Shared Hub ต่าง ๆ กัน เช่น VLAN1 มีสมาชิกจาก Segment ต่าง ๆ ดังนี้



รูปที่ 5
แสดงลักษณะของ Layer -3 VLAN

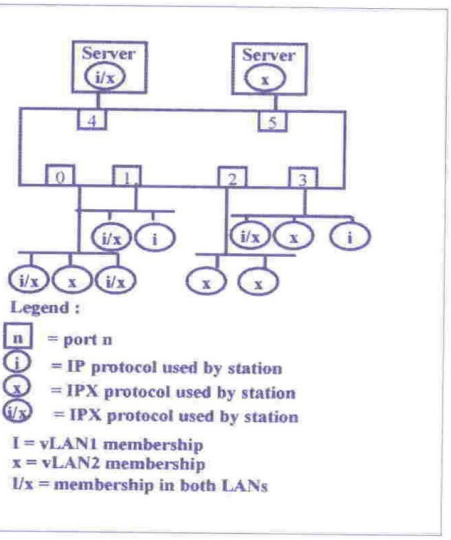
VLAN1 มีสมาชิก ประกอบด้วย 1, 2, 3, 4, 5, 6, 17
VLAN2 มีสมาชิก ประกอบด้วย 7, 8, 9, 19, 11, 12, 13, 14, 16, 18

Layer-3 Based VLAN

VLAN ประเภทนี้เป็นการกำหนด เลขหมายของ Subnet เป็นหลัก ดังนั้น การจัดแบ่ง VLAN ก็สามารถทำได้โดย กำหนดให้ VLAN แต่ละแห่งประกอบด้วย Subnet ต่างๆ ดังนั้น หากบนเครือข่ายมี 5 Subnet ก็จะสามารถแบ่ง VLAN ได้ 5 Subnet เช่นกัน ดังรูปที่ 5

Protocol Based VLAN

Protocol Based VLAN เป็นการกำหนด Protocol เป็นหลักในการเลือกสรรสมาชิกบน VLAN เช่น ผู้ใช้ที่ทำงานบน IP ก็ให้เป็นสมาชิก ของ VLAN1 ส่วนผู้ใช้ที่ทำงานบน IPX ก็ให้เป็นสมาชิกของ VLAN2 เป็นต้น (ดูรูปที่ 6)



รูปที่ 6 แสดงลักษณะการใช้งาน Protocol Based VLAN

Ruled- Based VLAN

บางครั้งจะเรียกว่า Policy Based VLAN เป็นระบบ VLAN ที่มองเข้าไปในตัว Packet หรือ Frame ที่วิ่งอยู่ภายในตัว Switching Hub โดยจะอาศัยข้อมูลที่อยู่ใน Packet หรือ Frame เป็นกลไกในการสร้าง VLAN ตัวอย่างเงื่อนไขการกำหนดสมาชิกของ VLAN ดังนี้

- IP User พร้อมด้วย IP Subnet Address เฉพาะเจาะจง เช่น 200.20.20.17-200.20.20.80 เป็นสมาชิก VLAN1 เป็นต้น
- IPX User ทั้งหมดพร้อมด้วย IPX Number Address เฉพาะเจาะจง
- ผู้ใช้งานบน Station ที่ใช้ LAN Card ของ 3Com
- ผู้ใช้งานที่มี Frame ซึ่งภายในใช้ Type Field เดียวกัน
- ผู้ใช้งานที่มี Frame ซึ่งภายในใช้ SNAP Field เหมือนกัน
- IPX Traffic ที่เกิดขึ้นทั้งหมดพร้อมด้วย Network Address จำเพาะแต่ยกเว้น Node Address เป็นพิเศษ

ที่กล่าวมาทั้งหมดนี้ เป็นวิธีการเพิ่มประสิทธิภาพการทำงานของเครือข่ายที่ใช้ Switching Hub ซึ่งจะเห็นได้ว่า ลำพังอาศัย Switching Hub ความเร็วสูงเพียงอย่างเดียวนั้นไม่เพียงพอ จึงต้องใช้เทคนิคการเชื่อมต่อต่างๆ ของ Switching Hub เข้าช่วยเพิ่มประสิทธิภาพของเครือข่าย

Non-Blocking Switch vs. Blocking Switch

เราเรียก Switch ที่เป็น Non-Blocking Switch ก็เป็นในกรณีที่ Switch Bus หรือ ส่วนประกอบของมันไม่สามารถรับมือกับ Theoretical Maximum Throughput ของ Input Port ทั้งหมดมารวมกัน หมายความว่า ระบบ Bus ภายในของ Switching Hub ไม่สามารถรับเอา Traffic จากพอร์ทต่าง ๆ ทั้งหมดของ Switching ไว้บน Bus ภายในได้หมด หรือความเร็วรวมทั้งหมดของพอร์ท เมื่อรวมกันแล้วมีมากกว่าความเร็วทั้งหมดของ Bus ภายใน

Internal Route Processor กับ External Route Processor

Routing ระหว่าง VLAN ด้วยกัน อาจมีปัญหาการสื่อสาร หากต้องการ Routing ระหว่าง VLAN ด้วยกัน ท่านจะต้อง ใช้ Layer 3 Route processor หรือ Router

มี Route Processor อยู่ 2 ประเภท ได้แก่

- External Route Processor
- Internal Route Processor

External Route Processor เป็นการใช้ External Router เพื่อแสวงหาเส้นทาง จาก VLAN หนึ่งไปอีก VLAN หนึ่ง ส่วน Internal Route Processor เป็นการใช้ Internal Modules และ Card ที่ติดตั้งอยู่ในอุปกรณ์เดียวกันเพื่อการ Routing ระหว่าง VLANs

มาตรฐาน โปรโตคอลการทำงานของ Switching Hub บน Cisco

Inter-Switch Link (ISL) Protocol

ISL Protocol เป็นโปรโตคอลสำหรับเครือข่าย Ethernet Switching ที่พัฒนาขึ้นโดย Cisco เป็นโปรโตคอลที่มีการเพิ่มข้อมูลขนาด 26 ไบต์ไปไว้ที่ส่วนหัวของ Ethernet Frame (ซึ่งผ่านการ Encapsulation มาเรียบร้อยแล้ว) รวมทั้งยังเพิ่มข้อมูลอีก 4 ไบต์ไว้ที่ส่วนท้ายซึ่งได้แก่ Checksum อีกด้วย จุดประสงค์หลักของ ISL ก็คือ การทำให้ทุก ๆ Frame บน เครือข่าย Ethernet ถูกบรรจุด้วยข้อมูลข่าวสารเกี่ยวกับ VLAN ในที่นี้จะเป็น VLAN ID No. ต่าง ๆ บนเครือข่าย และ Ethernet Frame ที่ประกอบด้วย VLAN ID No. นี้ จะถูกส่งผ่านไปมาระหว่างอุปกรณ์เครือข่ายของ Cisco ที่ถูกกำหนดให้เชื่อมต่อกันแบบ Trunking โดยเฉพาะ

ปัจจุบันมีผลิตภัณฑ์แลนการ์ดหลายรุ่นจาก Intel และบริษัทอื่น ต่างก็ให้การสนับสนุนการทำงานของ ISL Trunking ข้อดีก็คือสามารถนำมาเชื่อมต่อกับอุปกรณ์บนเครือข่าย Cisco และทำงานร่วมกันได้ แต่ถ้าหากว่าท่านต้องการใช้ VLAN Protocol ที่ไม่จำเพาะเจาะจงให้ใช้งานบนเครือข่ายของใครโดยเฉพาะ ท่านควรเลือกใช้ 802.1Q Protocol แทน (ดูรูปที่ 7)

ISL นอกจากจะเป็นโปรโตคอลเฉพาะกิจสำหรับระบบ Switching ของ Cisco แล้ว ISL ยังถูกนำมาใช้บน Trunk เพื่อเชื่อมต่ออุปกรณ์เครือข่ายที่ทำงานบน Fast Ethernet และ Gigabit Ethernet เท่านั้น โดย ISL จะทำหน้าที่หยอดใส่ข้อมูลข่าวสารเกี่ยวกับ VLAN ลงบน Frame ของ Ethernet ผ่าน แล้ววิ่งผ่าน Trunk ที่เชื่อมต่อระหว่าง Switch หรือ Router ของ Cisco

ข้อมูลที่ได้ หยอดใส่ ลงไปใน Ethernet Frame นี้ จะทำให้ VLAN ต่าง ๆ บนเครือข่าย ต่างก็จะรู้ว่า Frame ต่าง ๆ มาจาก VLAN ใดบ้าง หรือมาจากสมาชิกใน VLAN เดียวกันหรือไม่ ในกรณีที่บนเครือข่ายมี VLAN หลาย ๆ กลุ่มกระจายไปตาม Switching Hub ต่างๆ ที่เชื่อมต่อกันบน Trunk ตัว Frame ที่ผ่านการหยอดใส่ข้อมูลโดย ISL ก็จะสามารถถูกส่งออกไปที่ Trunk ในลักษณะของการสลับ Frame (Multiplexing) โดยที่จะไม่ก่อให้เกิด Traffic เพิ่มเติม บนเครือข่าย รวมทั้งไม่มีการเปลี่ยนแปลงข้อมูลข่าวสารอื่น ๆ อีก ข้อสำคัญอีกประการหนึ่งคือ ท่านยังสามารถใช้ ISL เพื่อการสร้าง Trunk เพื่อเชื่อมต่อระหว่าง Cisco Router ทั้งสองที่ Support ISL หรือระหว่าง Switch กับ Router และระหว่าง Switch กับ Server ที่ใช้ LAN Card ซึ่งสนับสนุนโปรโตคอล ISL

ISL เป็นกระบวนการหยอดใส่แล้วหนีบข้อมูลข่าวสารลงบน Ethernet Frame ประเภทกระทำจากภายนอก (External Tagging Process) โดยที่จะไม่มีการตกแต่งเปลี่ยนแปลงเฟรมของเดิมแต่อย่างใด การหนีบข้อมูลนี้ก็เป็นเพียงการเพิ่ม ISL Header ขนาด 26 ไบต์ รวมทั้งจะเป็นการเพิ่ม 4 ไบต์ Frame Check Sequence (FCS) ที่ด้านท้ายสุดของเฟรม

สิ่งที่จะต้องจำไว้คือมีเพียงอุปกรณ์ Cisco หรือ LAN Card ที่สนับสนุน ISL เท่านั้นที่สามารถเข้าใจความหมายของ Frame ที่ผ่านการหนีบใส่ข้อมูลด้วยวิธีการ ISL และ Frame ที่ผ่านกระบวนการ ISL จะมีขนาดที่เกินมาตรฐานของอีเธอร์เน็ตที่กำหนดให้ ขนาดเฟรมต้องไม่เกิน 1518 ไบต์ ต่อไปนี้ คือลักษณะของ Frame ที่ผ่านกระบวนการ ISL

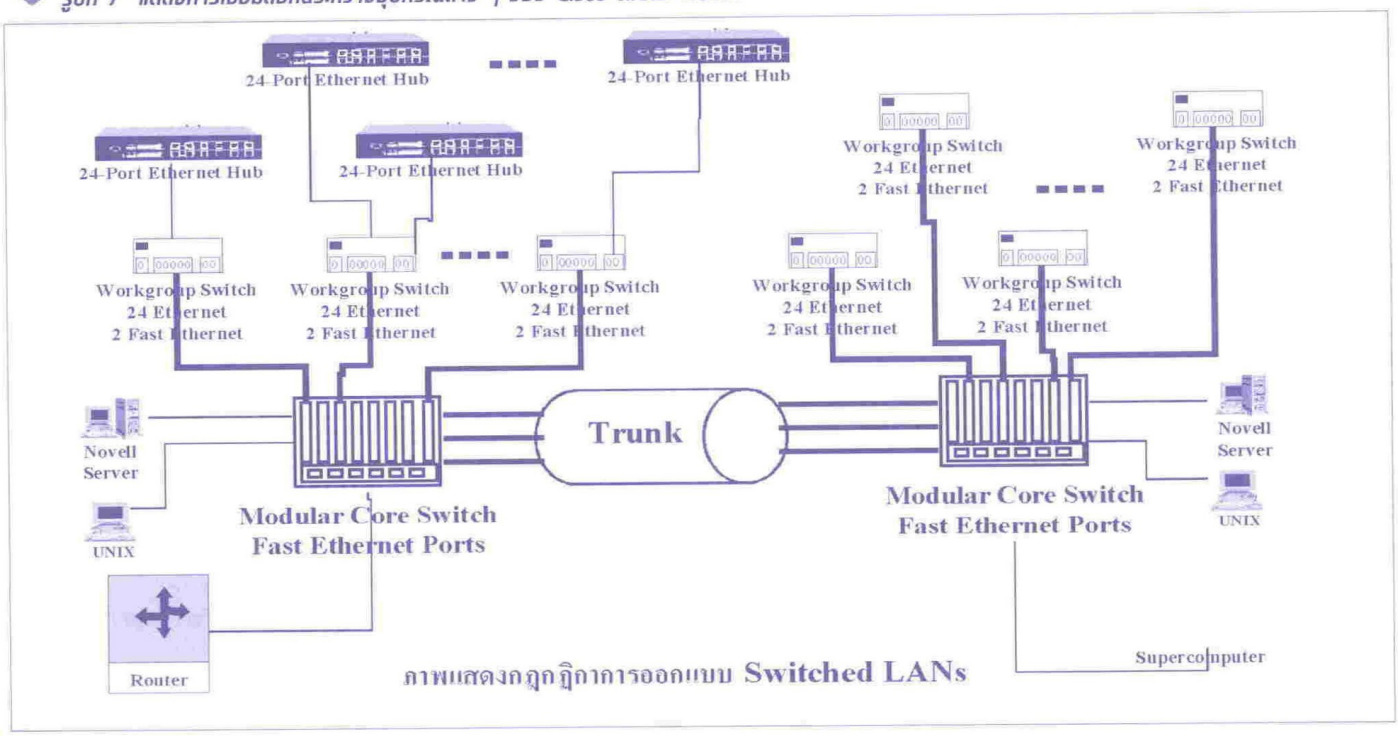
ISL Header	Encapsulated Frame	Frame Check Sequence

ISL Header มีขนาด 26 ไบต์ ประกอบด้วยข้อมูลข่าวสารเกี่ยวกับ VLAN บนเครือข่าย ส่วน Encapsulated Frame จะหมายถึง Ethernet Frame ดั้งเดิม ส่วน Frame Check Sequence (FCS) ก็เป็นส่วนที่ใช้ตรวจสอบความผิดพลาดเพิ่มเติมขนาด 4 ไบต์ สำหรับ ISL เท่านั้น

รูปแบบการเชื่อมต่อสำหรับเครือข่าย Switching LAN ขนาดใหญ่

รูปแบบการเชื่อมต่อเครือข่าย Switching LAN ขนาดใหญ่ ที่ได้รับการยอมรับจากนักออกแบบเครือข่ายทั่วไป มาจากแนวคิดของผู้ผลิต อุปกรณ์ Switching Hub รายใหญ่ เช่น Cisco เป็นต้น ซึ่งมีสาระการเชื่อมต่อดังนี้(ดูรูปที่ 8 ประกอบ)

รูปที่ 7 แสดงการเชื่อมต่อกันระหว่างอุปกรณ์ต่าง ๆ ของ Cisco โดยใช้ Trunk



ภาพแสดงกฎกฎิกาการออกแบบ Switched LANs

- Access Layer Switches
- Distributed Layer Switches
- Core Layer Switches

Access layer Switches

Access Layer เป็นระดับที่มีความสำคัญเนื่องจากเป็นจุดที่ผู้ใช้งานบนเครือข่าย อาศัยจุดนี้เพื่อการ Access เข้าสู่เครือข่าย อุปกรณ์การเชื่อมต่อที่ใช้ในจุดนี้ ได้แก่ Shared Hub หรือ Switching Hub หรือทั้งสองอย่างรวมกัน โดยทั่วไปจุดนี้ จะเป็นจุดที่ผู้ใช้งานต่างก็แบ่งใช้งาน Bandwidth นอกจากนี้การจัดตั้ง VLAN พร้อมด้วยสมาชิกก็เกิดขึ้นที่นี่ เช่นกัน

เป้าหมายหลักของระดับการเชื่อมต่อจุดนี้ได้แก่ การส่งผ่านการสัญจร (Traffic) ของข้อมูลข่าวสารไปที่เครือข่ายสำหรับผู้ใช้งาน รวมทั้งการกลั่นกรองข้อมูลข่าวสารที่ไม่เกี่ยวข้องกับผู้รับปลายทาง

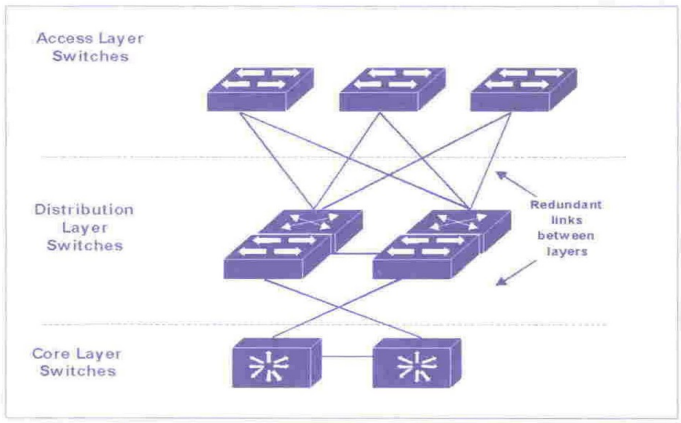
Switching Hub ที่ติดตั้ง ณ บริเวณนี้ทำหน้าที่เชื่อมต่อระหว่างสายสัญญาณของผู้ใช้งานกับ Switching Hub ขณะที่อีกด้านหนึ่ง ก็มีการเชื่อมต่อทางกายภาพระหว่าง Switching Hub ในระดับ Access Layer กับ Switching Hub ในระดับ Distributed Layer และ Switching Hub ใน Access Layer นี้ มักจะเป็น Desktop Switching Hub ที่มี Port เพื่อการเชื่อมต่อตั้งแต่ 12-24 Port เท่านั้น (ดูรูปที่ 9)

Distributed Layer

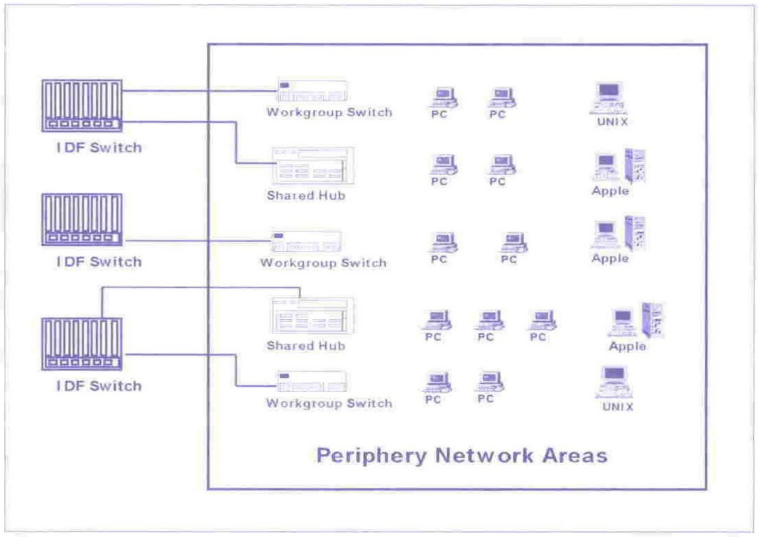
Distributed Layer เป็นจุดรวมการเชื่อมต่อจาก Switching Hub ในระดับ Desktop ต่างๆ การเชื่อมต่อในระดับชั้นนี้ยังประโยชน์หลายประการสำหรับเครือข่าย เช่น

- ประโยชน์ในด้านรักษาความปลอดภัย เนื่องจากสามารถจัดการเกี่ยวกับระบบรักษาความปลอดภัยได้จากที่นี่ นอกจากนี้ยังเป็นจุดที่สามารถเฝ้าดูการเข้าสู่เครือข่ายของผู้ใช้งานได้
- เป็นจุดที่ใช้เชื่อมต่อระหว่าง VLAN รวมทั้งจัดหาเส้นทางเพื่อติดต่อระหว่าง VLAN ต่างๆ
- เป็นจุดที่รวมเอาการเชื่อมต่อต่าง ๆ เข้าหากัน หมายความว่า เป็นจุดที่มีการติดตั้ง Switching Hub ที่มีขนาดใหญ่ มี Port ความเร็วสูงเป็นจำนวนมากเพื่อรองรับการเชื่อมต่อที่มาจาก Desktop Switching Hub ต่างๆ อีกทั้งใช้เป็นที่ ๆ ผู้ใช้งานต่างๆต้องการติดต่อกับ Server ด้วยความเร็วสูง

Switching Hub ที่ใช้เชื่อมต่อในระดับนี้จะเป็น Switching Hub ที่มีขนาดใหญ่ มีพอร์ทจำนวนมาก มี Port Trunking หรือ Fat Pipe สามารถมี MAC



รูปที่ 8 แสดงการจัดแบ่งรูปแบบการเชื่อมต่อของ เครือข่าย Switching ในลักษณะ Layer



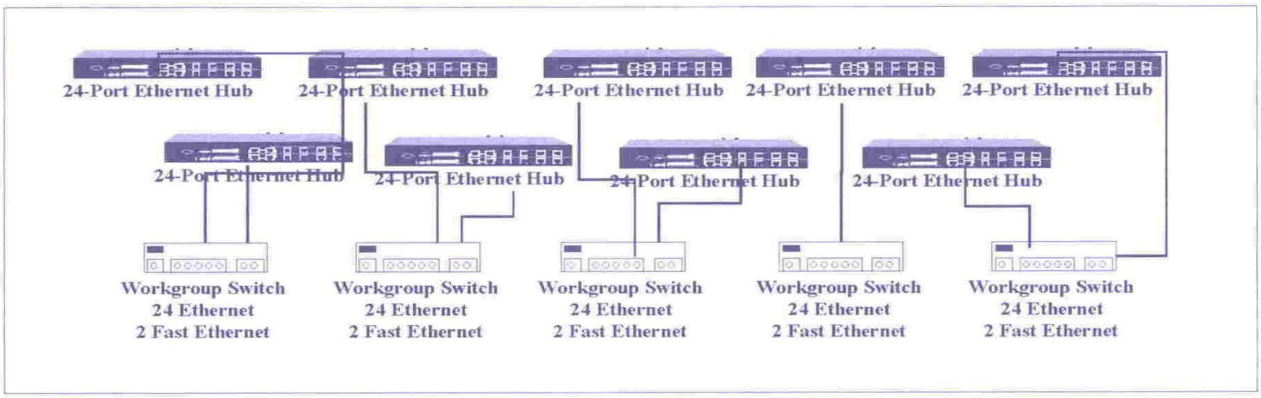
รูปที่ 9 แสดงลักษณะการเชื่อมต่อในระดับ Access Layer

Address ได้มากถึง 2-3 พัน MAC Address หรือมากกว่า นอกจากนี้ ยังมี Uplink Port ความเร็วสูง ไว้เพื่อเชื่อมต่อกับ Desktop Switching Hub ต่างๆ อีกด้วย และที่สำคัญ มักจะเป็น Layer 3 Switch รวมทั้งสนับสนุน ระบบบริหารจัดการและเฝ้าดู และ Alarm เตือนเครือข่าย เมื่อเกิดปัญหา ค่าที่ตั้งไว้เกินพิกัด เช่น SNMP v2 หรือ RMON อีกด้วย

รูปแบบการเชื่อมต่อในระดับ Distributed Layer มีดังนี้ (ดูรูปที่ 10)

Core Layer

Core Layer เป็นระดับชั้นการเชื่อมต่อที่มีหน้าที่อยู่อย่างเดียว แต่ทำได้มากกว่าหนึ่งอย่าง หน้าที่หลักได้แก่การทำหน้าที่ Switch ตัว Frame หรือ Packet อย่างเร็วที่สุดเท่าที่จะเร็วได้ อีกทั้งยังเป็นจุดสุดท้ายที่รวมการเชื่อมต่อของผู้ใช้งานจาก Station ต่าง ๆ ผ่านมาทาง Distributed Layer เพื่อเชื่อมออกไปจากเครือข่ายไปยังเครือข่ายอื่น ๆ

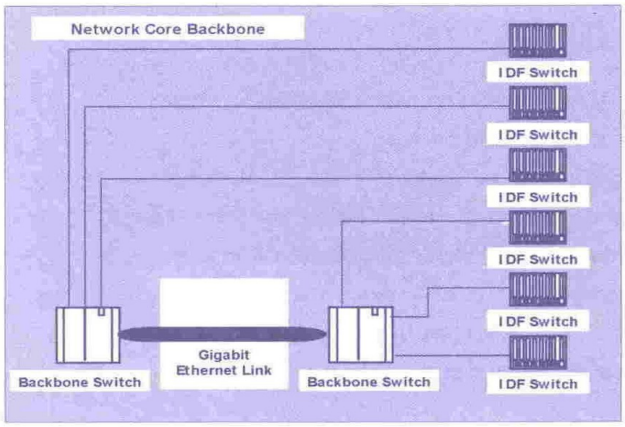


รูปที่ 10 แสดงลักษณะการเชื่อมต่อบน Distributed Layer

ในส่วนของ Core Layer นี้ จะไม่มีการตัดสินใจเกี่ยวกับ การกลั่นกรอง Packet รวมทั้งจะไม่มีการจัดหาเส้นทางเดินให้กับ Packet เนื่องจากว่า การที่ Core Layer ต้องมีหน้าที่ส่งผ่าน Packet ให้เร็วที่สุดเท่าที่จะทำได้ ทำให้ Core Layer ไม่สามารถแบกรับภาระในเรื่องของ Delay หรือ Latency ได้ นอกจากนี้การเกิด Error ที่จุดนี้ จะมีผลต่อการทำงานของเครือข่ายโดยรวม

Switching Hub ที่ติดตั้งอยู่ในระดับนี้ มักจะเป็น Enterprise Switches บางครั้งจะเรียกว่า Edge Switches เป็น Switches ที่เชื่อมต่ออยู่กับแกนหลักของเครือข่าย มีความเร็วสูง อาจเชื่อมต่อกับ Core Switches อื่น ๆ โดยทาง Gigabit Ethernet Interface หรืออาจใช้ ATM OC3 ก็ได้

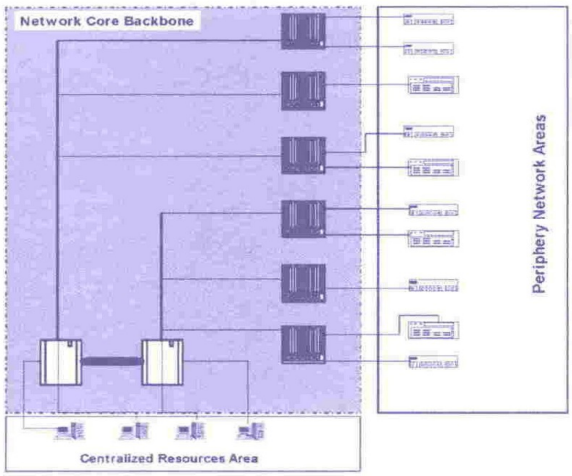
รูปแบบการเชื่อมต่อของ Core Layer มี ดังนี้ (ดูรูปที่ 11)



รูปที่ 11 แสดงการเชื่อมต่อบน Core Layer

การออกแบบเครือข่าย Switched

การออกแบบเครือข่าย Switched LAN จำเป็นต้องกำหนดระดับของการเชื่อมต่อ ซึ่งบางครั้งจะเรียกว่าพื้นที่อาณาบริเวณ หรือ Area ซึ่งท่านสามารถใช้แนวคิดการเชื่อมต่อเป็นระดับได้ 3 ระดับ ต่อไปนี้ เรามาดูตัวอย่างการออกแบบ ของอาคารสำนักงานแห่งหนึ่งที่ประกอบด้วย เครือข่ายขนาดกลางดังต่อไปนี้ (ดูรูปที่ 12)



รูปที่ 12 แสดงตัวอย่างการเชื่อมต่อของเครือข่าย Switched LAN สำหรับสำนักงาน

จากรูปที่ 12 จะเห็นว่าการออกแบบเครือข่าย Switched LAN จำเป็นต้องมีการกำหนดพื้นที่การเชื่อมต่อออกเป็นอย่างน้อย 3 ส่วนหลัก ๆ สำหรับเครือข่ายขนาดกลาง หรือขนาดใหญ่ โดยเฉพาะการเชื่อมต่อเครือข่ายภายในอาคารที่กระจายไปตามชั้น (Floor) ต่าง ๆ ของอาคารทั้งขนาดกลางและขนาดใหญ่อย่างเช่น ตึก World Trade ผู้ล่วงลับ ไปแล้วก็ตาม รวมทั้งยังเหมาะสำหรับ การเชื่อมต่อระหว่างอาคารอีกด้วย

การจัดแบ่งพื้นที่การเชื่อมต่อ จะช่วยให้เกิดประโยชน์มากมายหลายประการ ได้แก่

- การบริหารจัดการเป็นไปได้โดยง่ายโดยท่านอาจเลือกใช้ซอฟต์แวร์ประเภท Network Management หรือ RMON ไว้ที่ Switches Hub ตัวใดตัวหนึ่ง ณ จุดใดจุดหนึ่ง หรือหลายๆ จุดก็ได้ ทำให้สามารถตรวจสอบปัญหา

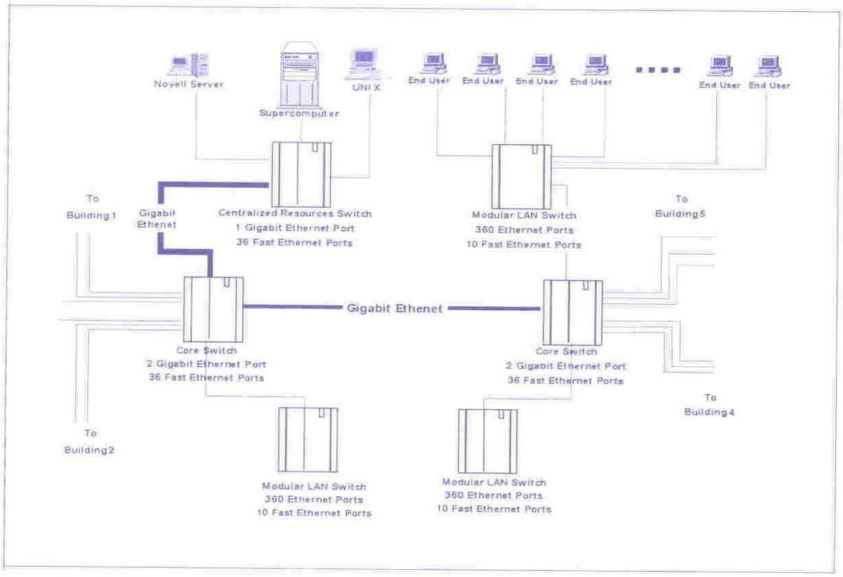
ที่เกิดขึ้นได้ง่าย เนื่องจากท่านสามารถดูปัญหาที่เกิดขึ้นได้เป็นจุด ๆไป อีกทั้งยังสามารถควบคุมดูแลปริมาณของ Traffic ในแต่ละจุดมิให้มีมากเกินไป และหากมีมากเกินไป ก็สามารถกำหนดให้มีการเตือนเป็นจุด ๆ ไปได้อีกด้วย

- สามารถขยายขนาดของเครือข่ายได้โดยง่าย (Scalability) การแบ่งพื้นที่ก็คล้ายกันกับการเชื่อมต่อที่แบ่งออกเป็น Modules โดยที่ท่านสามารถขยายหรือลดขนาดของ Modules โดยไม่กระทบกระเทือนเครือข่ายแต่อย่างใด นอกจากนี้ยังช่วยให้สามารถเลือกซื้ออุปกรณ์ที่เหมาะสมสำหรับแต่ละ Modules อีกด้วย
- สามารถควบคุมดูแลรักษาความปลอดภัยได้ดี เนื่องจากเป็นลักษณะของ Modules ทำให้เป็นเรื่องง่ายที่จะกำหนดพื้นที่อาณาบริเวณ เพื่อควบคุมดูแลรักษาความปลอดภัยได้โดยง่าย
- มี Network Availability สูง คำว่า Network Availability หมายถึงขีดความสามารถที่ระบบเครือข่ายสามารถให้บริการแก่ผู้ที่จะเข้ามาใช้งานมากที่สุดหรืออย่างต่อเนื่อง โดยมีค่าหน่วงเวลา (Delay หรือ Latency) น้อยที่สุด ซึ่งการเชื่อมต่อแบบพื้นที่อาณาบริเวณแบบนี้จะช่วยให้ สามารถควบคุม Bandwidth ได้ดี รวมทั้งสามารถควบคุม Traffic ได้อีกด้วย นอกจากนี้ทำให้ท่านสามารถเลือกหรือกำหนดให้ มีการจัดตั้ง Redundancy Link เพื่อหลีกเลี่ยง การล่มสลายแบบถอนรากของเครือข่าย (Single Point of Failure)
- มีประสิทธิภาพสูง เนื่องจากการกำหนดพื้นที่การเชื่อมต่อ ทำให้ต้องมี Back Bone เพื่อเชื่อมต่อระหว่าง Switches ต่างๆ ซึ่ง Back Bone นี้ ท่านอาจเลือกใช้ Gigabit หรือ ATM OC-3 Link ก็ได้

พื้นที่การเชื่อมต่อ

พื้นที่การเชื่อมต่อ สำหรับเครือข่าย Switched LAN สามารถแบ่งออกเป็น 3 ส่วนได้ดังนี้

- พื้นที่ในส่วนที่เป็นแกนของการเชื่อมต่อ (Core Area)
- พื้นที่ในส่วนของ อุปกรณ์เชื่อมต่อเครือข่าย (Periphery Network Area)
- พื้นที่ในส่วนของศูนย์ จัดเก็บข้อมูล (Centralized Resource Area)



รูปที่ 13 แสดงส่วนประกอบหลักของพื้นที่ส่วนที่เป็นแกน

พื้นที่ในส่วนที่เป็นแกนของการเชื่อมต่อ (Core Area)

บางครั้งจะเรียกว่าเป็น Core หรือ Back Bone ก็ได้ ส่วนที่เป็น Core นี้ประกอบไปด้วย 2 ส่วน ได้แก่ ส่วนที่ประกอบด้วย Back Bone หรือ Core Switches และส่วนที่เป็นสาย Back Bone พร้อมด้วย Switches ที่เชื่อมต่อระหว่าง Floor ดังรูปที่ 13

พื้นที่ส่วนที่เป็นแกนหลักนี้จัดเป็นพื้นที่สำคัญและล่อแหลมที่สุด ณ จุดนี้จะเป็นจุดรวมการเชื่อมต่อจากผู้ใช้งาน ใน Floor ต่างๆ ทั้งหมด ดังนั้นจุดที่เป็น Core นี้จะต้องมีคุณลักษณะที่สำคัญ 2 ประการ ได้แก่ จะต้องมีประสิทธิภาพสูงยิ่ง และต้องมี Redundancy สูง รวมทั้ง Fault Tolerance เช่นกัน ซึ่งแน่นอนค่าอุปกรณ์ Switches ณ จุดนี้ย่อมมีราคาแพงมาก

จากรูปที่ 13 จะเห็นว่าการเชื่อมต่อในพื้นที่ Core นี้ประกอบด้วย Backbone Switch 1 ตัวหรือมากกว่า โดยทำหน้าที่เป็นจุดศูนย์กลางของเครือข่าย Switched หรือบางทีก็เรียกว่า Main Distribution Frame (MDF) ซึ่งใช้สายสัญญาณ Backbone ความเร็วสูง ที่อาจทำจากสาย Fiber Optic เพื่อเชื่อมต่อกับ IDF Switches โดย IDF Switches ทำหน้าที่ดูแลการเชื่อมต่อเข้ามาของ Switching Hub หรือ Shared Hub ในแต่ละ Floor โดย Core Area นี้ จะใช้ IDF Switches เพื่อเชื่อมต่อกับพื้นที่ Periphery Area

ลักษณะของสาย Backbone จะต้องเป็นสาย Fiber Optic ที่มีความเร็วสูงเพื่อเชื่อมต่อระหว่าง Core Switches กับ IDF Switches และการเชื่อมต่อระหว่าง Core Backbone Switches จะเป็นรูปแบบ Port Trunking โดยท่านอาจเลือก การเชื่อมต่ออย่างใดอย่างหนึ่งได้ดังต่อไปนี้

- 100Base-FX แบบ Full Duplex
- Gigabit Ethernet
- ATM OC3 (155 Mbps)
- ATM OC12 (622 Mbps)

การเชื่อมต่อจะต้องมี Back Up Link หากการเชื่อมต่อจุดเส้นใดเส้นหนึ่งมีปัญหา ก็สามารถใช้อีกเส้นหนึ่งแทนได้ ทันที เราเรียกว่า Redundancy Link

นอกจากนี้ตัว Core Switches จะต้องมีระบบจ่ายไฟในตัวถึง 2 ชุด (N+1 Power) ซึ่งหากระบบจ่ายไฟเกิดมีปัญหา ระบบจ่ายไฟอีกชุดจะทำงานแทนที่โดยอัตโนมัติ

นอกจากนี้ท่านอาจต้องมี Backbone Switches ถึง 2 ตัว ในกรณีที่ต้องรับภาระ Load ขนาดใหญ่มาก เช่น ในอาคารนี้อาจมีคอมพิวเตอร์ความเร็วสูง และความเร็วปานกลางหลายร้อยหรือกว่าพันเครื่องขึ้นไป การใช้ Backbone Switches เพียงชุดเดียวอาจไม่พอก็ได้ และเมื่อมีการใช้ Backbone Switches มากกว่า 1 ตัวขึ้นไป ให้พิจารณาการเชื่อมต่อระหว่าง Backbone Switches ทั้งสอง โดยเลือกการเชื่อมต่อแบบเดียวกันกับการเชื่อมต่อระหว่าง Backbone Switches กับ IDF Switches

ข้อกำหนดสำหรับ Core Area

Core Area จะต้องมีลักษณะพิเศษดังนี้

1. จะต้องมีประสิทธิภาพความเร็วสูง
2. จะต้องมีสายสัญญาณเชื่อมต่อแบบ Backup Link ในรูปแบบของ Loop (ดังที่เคยอธิบายในฉบับก่อนหน้านี้
3. จะต้องมีระบบจ่ายไฟในตัว Backbone Switches ที่สามารถทำงานโดยอัตโนมัติ เมื่อใดที่ระบบจ่ายไฟตัวหนึ่ง ไม่ทำงาน
4. จะต้องสามารถใช้ Port Trunking เพื่อการเชื่อมต่อความเร็วสูงได้
5. Backbone Switches จะต้องมีปริมาณของ Port มากพอที่จะรองรับการเชื่อมต่อกับ IDF Switches ได้ รวมทั้งการรองรับการขยายในอนาคตอีกด้วย

พื้นที่ของศูนย์จัดเก็บข้อมูล

เป็นที่ตั้งของ Resource ต่าง ๆ เช่น Server Router หรือ Internet Firewall Mainframe และอุปกรณ์เก็บข้อมูลอื่น ๆ ที่ผู้ใช้งานจะต้องเข้ามาใช้งานเป็นประจำ Server ณ พื้นที่บริเวณนี้ อาจเป็น Web Server/Email Server FTP Server ซึ่งมักถูกเรียกว่า Enterprise Server ลักษณะพิเศษของ Centralized Resource Area นี้ มีจุดที่น่าสนใจหลายประการ

- หากมี Server เป็นจำนวนมาก ท่านอาจต้องพิจารณาเลือกติดตั้ง Switching Hub อีกตัวหนึ่งเพื่อเชื่อมต่อกับ Backbone Switches โดยเฉพาะ ทั้งนี้ก็เพื่อลดจำนวนสายสัญญาณเชื่อมต่อระหว่าง Server กับ Backbone Switches ซึ่งก็หมายถึงการประหยัด Port ที่ Backbone Switches รวมทั้งค่าใช้จ่ายอีกด้วย
- สายสัญญาณ Up Link ที่เชื่อมต่อระหว่าง Switches กับ Backbone Switches จะต้องมีความเร็วสูง

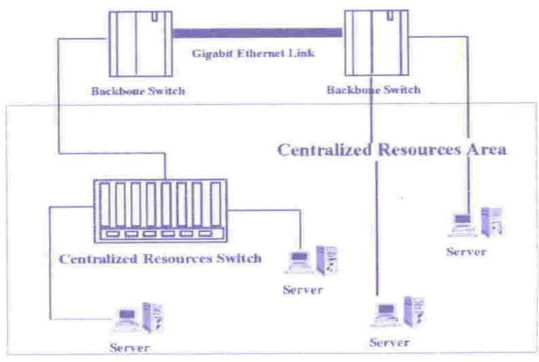
สำหรับคุณลักษณะของ Centralized Resource Area มีดังนี้

1. **สามารถบริหารจัดการได้ง่ายและสะดวก** ต้องมีการติดตั้ง RMON (Remote Monitoring) รวมทั้ง Alarm เตือนที่ต้องติดตั้งบน Centralized Resource Area Switches
2. **ให้การสนับสนุนการเชื่อมต่อแบบ Full Duplex** เนื่องจากว่าจะมี Traffic ในปริมาณมากวิ่งผ่านมาที่ Switches เหล่านี้ การใช้ Full Duplex จึงมีความจำเป็นมาก ทำให้ข้อมูลสามารถวิ่งไปและ กลับในเวลาเดียวกัน ซึ่งทำให้เกิดประโยชน์หลายประการ ดังนี้
   - ทำให้มีการรับส่งข้อมูลเป็นทวีคูณ บนการเชื่อมต่อแบบจุดต่อจุด (Point to Point)
   - ช่วยลดหรือขจัด Collision ลงได้ทำให้สามารถลดอัตราการเกิด Retransmission ลงได้
3. **ปริมาณของ Port ความเร็วสูงมากพอ** ตัว Switches ที่ใช้เชื่อมโยงระหว่าง Centralized Resource กับ Network Core Backbone จำเป็นต้องใช้ Interface ความเร็วสูงจำนวนหนึ่ง และPort ของ Switches เหล่านี้ จะต้องมีความเร็วสูง เพื่อใช้เชื่อมต่อ Server ความเร็วสูง เช่น 100 Mbps หรือสูงกว่า แต่ในบางกรณีท่านอาจเลือกใช้ Centralized Resource Switches เพื่อลดจำนวนของ สายสัญญาณระหว่าง Backbone Switches กับ Centralized Resource ก็ได้
4. ความน่าเชื่อถือของระบบ ในกรณีที่ Periphery Switches เกิดล้มเหลว ผู้ใช้งานทุกคนบนเครือข่าย อาจได้รับผลกระทบ ดังนั้น Switches ที่เชื่อมต่อกับ Server จะต้องมีความน่าเชื่อถือ

   โดยจะต้องมีปัจจัยพื้นฐานได้แก่ N+1 Redundant Power (ระบบจ่ายไฟชุดที่สอง ที่จะทำงาน

   โดยอัตโนมัติ หากระบบไฟชุดแรกไม่ทำงาน)
5. มี Up Link Trunking ความเร็วสูง เนื่องจาก Switches เหล่านี้เป็นจุดรวมของ Traffic ขนาดใหญ่ ดังนั้นการเชื่อมต่อไปที่ Core จะต้องมี Capacity สูง โดยการเลือก Switches ที่มี Trunking Capacity สูง เช่น Port Trunking เป็นต้น

รูปแบบการเชื่อมต่อของ Centralized Resource Area มีดังนี้ (ดูรูปที่ 14)



รูปที่ 14 แสดงลักษณะการเชื่อมต่อบน Centralized Resource Area

พื้นที่ในส่วนของ อุปกรณ์เชื่อมต่อเครือข่าย Periphery Area

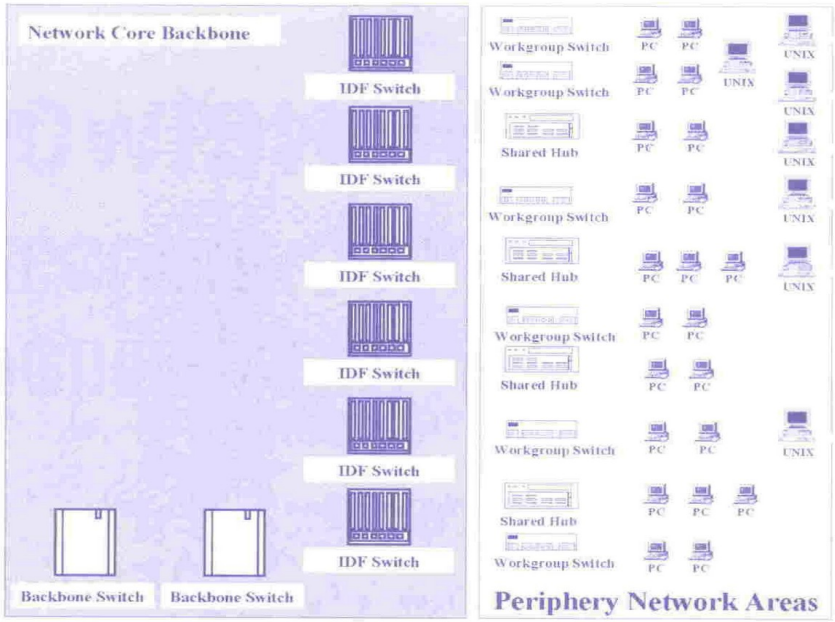
เป็นพื้นที่สำหรับผู้ใช้งาน ซึ่งพื้นที่บริเวณนี้ ต้องการ Switched Port เป็นจำนวนมาก เพื่อรองรับจำนวนของผู้ใช้งาน เป็นจำนวนมากเช่นกัน

ภายใน Periphery Area ของ Switched LAN นี้จะมีอุปกรณ์ที่ติดตั้งอยู่ 2 ประเภท ได้แก่

1. Workgroup Switches เชื่อมต่อระหว่างผู้ใช้งานกับ Switches Port โดยตรง ซึ่ง Switches Port เหล่านี้ อาจเป็นในรูปแบบ Stackable หรือแบบ Modular Chassis อย่างใดอย่างหนึ่ง
2. Shared Access Hub เป็น Repeater Hub ทั้งแบบ Stackable หรือ Modular

คุณลักษณะจำเพาะสำหรับ Periphery Area

- จำนวนของ Port ที่ใช้เชื่อมต่อกับผู้ใช้งานจะต้องมีมากพอหรือให้มีมากที่สุด เนื่องจากว่าการมี Switches ที่มีพอร์ทมากจะทำให้สามารถลดจำนวนการใช้ Switches หลายๆตัว ซึ่งจะส่งผลให้ต้องเพิ่มพอร์ทที่ IDF Switches ซึ่งมีราคาแพง พูดง่าย ๆ คือการเลือกซื้อ Switches ที่มี Port มาก ๆ ยังดีกว่าซื้อ Switches หลาย ๆ ตัว
- ความสามารถในการขยาย ตัว Switches จะต้องสามารถเพิ่มขยายจำนวนของผู้ใช้งานได้มาก ๆ ซึ่งไม่เพียงแต่จะเพิ่มจำนวน Port ได้มากขึ้นแล้ว อาจต้องพิจารณาเรื่องขีดความสามารถในการเพิ่ม Up Link อีกด้วย
- ประสิทธิภาพของ Up Link Port ตัว Switches จะต้องมี Up Link Port อย่างน้อยหนึ่ง Port อัตราความเร็วของ Up Link Port นี้ อย่างน้อยต้อง 100 Mbps ขึ้นไป สายที่ใช้ควรเป็น Fiber Optic
- ความสามารถในการจัดการเครือข่ายตัว Switches จะต้องติดตั้ง SNMP v2 หรือ RMON อย่างใดอย่างหนึ่ง ทั้งเพื่อเฝ้าดูกิจกรรมภายในเครือข่ายเฉพาะในส่วนของ Periphery Area เท่านั้น ลักษณะการเชื่อมต่อภายใน Periphery Area มีดังนี้ (ดูรูปที่ 15)



รูปที่ 15 แสดงลักษณะการเชื่อมต่อภายใน Periphery Area

ข้อแนะนำสำหรับการออกแบบ Switched LAN

องค์กรทั่วไปที่มีจำนวนคอมพิวเตอร์ไม่มาก เช่น เครือข่ายขนาดเล็กใช้เพียง Desktop Switching ขนาด 24 พอร์ทเชื่อมต่อกับฮับต่าง ๆ ก็เพียงพอแล้ว สำหรับท่านที่ต้องการความปลอดภัย และได้แบนวิดธ์ในการทำงานที่ดีและเผื่อที่จะขยายในอนาคต ก็ควรเลือกใช้ Switches ที่สนับสนุนระบบ VLAN นอกจากนี้ยังต้องมี Up Link Port ที่สนับสนุน100Base-FX หรือ Gigabit 1000Base-SX สำหรับองค์กรที่มีคอมพิวเตอร์เป็นจำนวนมากกระจายไปตาม Floor ต่าง ๆ และมี Shared Hub เป็นจำนวนมากในแต่ละ Floor ควรเลือกรูปแบบการเชื่อมต่อที่ผู้เขียนนำเสนอในบทนี้

เนื่องจากเนื้อหาของบทความ Switches ที่สามารถเขียนได้เป็นหนังสือหนึ่งเล่มใหญ่ และเนื่องจากเนื้อที่บทความจำกัดผู้เขียนไม่สามารถนำมาเสนอท่านได้เต็มที่ แต่ก็มั่นใจว่าท่านผู้อ่านคงได้รับสาระบันเทิงโดยทั่วกัน

หากท่านผู้อ่านท่านใดมีข้อสงสัยหรือ คำแนะนำเพิ่มเติมเกี่ยวกับบทความนี้ สามารถติดต่อได้ที่ **http://www.cyberthai.com**